



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 27 June 2005

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Los Angeles Times reports aircraft at Los Angeles International Airport came too close four times in the last month, a spate of incidents that officials attributed to human error and a record number of international flights. (See item [8](#))
- Knight Ridder reports a federal crackdown on fraud at state motor vehicle departments across the country has apprehended more than a dozen illegal immigrants licensed to transport hazardous materials. (See item [10](#))
- The Government Accountability Office has issued a report entitled, "Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism," which discusses protecting federal property assets under the threat of terrorism. (See item [24](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)
Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)
Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)
Federal and State: [Government](#); [Emergency Services](#)
IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)
Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 26, Chicago Sun-Times* — **Large blackout affects Chicago.** Utility ComEd restored power Saturday, June 25, to the last of its customers still without electricity from an outage caused by a fire in a South Side vault. The outage, which began around 8:30 p.m. Friday, June 24, affected 51,000 customers in the area from Hubbard Street to 49th Street and Lake Shore

Drive to Western Avenue. By 5 p.m. Saturday, ComEd had restored power to all but 6,800 customers. By 8:15 p.m., power was completely restored, officials said. ComEd said it was still unclear what caused the fire that shut down two 138-kilovolt power lines at the utility's Fisk substation, near 22nd and Racine. ComEd shut down additional power lines to allow firefighters to attack the flames, which shot as high as 15 feet. ComEd President Frank Clark said there was no evidence of a power surge, but the utility reported near-peak energy usage by its 3.7 million customers Friday, when temperatures reached 96 degrees.

Source: <http://www.suntimes.com/output/news/cst-nws-outage26s1.html>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

2. *June 26, U.S Chemical Safety and Hazard Investigation Board* — **CSB team tours site of St. Louis gas explosion accident.** A team from the U.S. Chemical Safety and Hazard Investigation Board (CSB) arrived in St. Louis, MO, on Saturday, June 25, to get a first-hand look at the damage wreaked by Friday's multiple gas explosions at the Praxair Inc. facility. CSB Investigation Manager Steve Selk, who led the team of three, toured the plant and surrounding community to assess the damage and impact of the incident. Praxair handles propane, acetylene and other gases for sale to industrial and commercial customers, the tanks of which generated the sequence of fiery explosions seen during the incident. In addition to the charred debris covering the grounds of the facility, investigators found nearby homes, buildings and cars that were struck and burned or damaged by airborne cylinders hurtled offsite. In one case, a two-foot diameter hole was found in the brick wall of a residence. Large, twisted pieces of metal were also found on the grounds and gardens of nearby residences and there was evidence of small fires that were ignited off-site. "The sheer volume of cylinders exploding, which numbered in the hundreds, certainly concerns us. The CSB's role in these types of accidents is aimed at preventing them from happening again," said Selk.

Source: http://www.csb.gov/index.cfm?folder=news_releases&page=news&NEWS_ID=230

3. *June 24, Cecil Whig (MD)* — **Chemical fumes injure five causing Maryland county landfill to evacuate.** The Cecil County, MD Landfill was evacuated Wednesday, June 22, after five workers were exposed to a hazardous chemical found in a load of trash. Those exposed, all county employees, were decontaminated before being treated at Union Hospital and later released. Exposure to the chemical, identified by officials as methylene chloride, a carcinogen, can cause difficulty breathing, nausea, vomiting, chemical burns and other health effects, according to the Agency for Toxic Substances and Disease Registry. The chemical arrived at the landfill in a 55-gallon drum Wednesday, June 22, said Department of Public Works Director Matheu Carter. Two equipment operators discovered the drum mixed in with a load of trash being dumped from a truck shortly after noon and called a supervisor, Carter said. About 40 emergency workers, including hazardous materials units from Harford County and the Maryland Department of the Environment spill response team, converged on the landfill. The landfill was shut down for the day. Officials determined the drum, which was nearly empty at the time, was inadvertently placed into a Dumpster by Colonial Metals Incorporated of Elkton, MD. The solid waste and environmental crimes unit of the Maryland Department of the Environment is investigating.

Source: <http://www.cecilwhig.com/articles/2005/06/23/news/01.txt>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

4. *June 24, TNA* — **Banks issue chip card to counter identity theft.** Thailand's commercial banks plan to replace their existing magnetic cards with those containing a computer chip by next year. In the meantime, the banks have tightened surveillance because of reports of identity theft. The new chip cards will offer better protection against data theft, according to Choke Na Ranong, Bangkok Bank's credit card manager. Thailand is increasingly vulnerable to credit card fraud as scammers move there from Malaysia where chip cards have already replaced the magnetic kind, according to Somchai Pichitsorakit, a senior executive at Thailand's second largest bank Kasikorn Bank. The Kasikorn Bank plans to introduce their chip cards by the end of 2005. The state-owned Krung Thai Bank, with more than a million credit cards in circulation, has announced it will issue chip cards by 2006. Most banks in Thailand plan to speed up the issue of chip cards, as they are the most effective deterrent against fraud, according to Thammasak Jittimapon, a senior executive at the Bank of Asia.

Source: <http://etna.mcot.net/query.php?nid=39604>

5. *June 24, Netcraft (UK)* — **New phishing attacks eliminate need for target Website.** New phishing attacks with data collection forms embedded directly in the electronic mails received by victims are inducing victims to send their financial details directly to the phishers via mail rather than through a specially constructed Website mimicking that of the financial institution. Phishing typically collects data through a Website that imitates a bank or online retailer. By including the data collector in an HTML email, the new attack eliminates a step in the process, allowing phishing scams to steal sensitive information without constructing an elaborate fraudulent Website. The HTML form within the e-mail lets phishers set the destination e-mail address, allowing for easy re-routing of submissions as mailboxes are shut down. The scam takes advantage of known insecurity in Formmail, a widely used form-to-mail Perl script initially written in 1995. In early 2001, spammers began using Formmail to anonymously deliver massive volumes of spam, taking advantage of the Formmail's failure to restrict access to the script. Most hosting providers have replaced the original Formmail with customized versions or secure replacement scripts like the NMS Project, although there are exceptions.

Source: http://news.netcraft.com/archives/2005/06/24/new_phishing_at_tacks_eliminate_need_for_target_web_site.html

6. *June 24, CNET News.com* — **ChoicePoint overhaul falls behind.** ChoicePoint, the data broker that leaked the personal information of 145,000 Americans, has gone off schedule in its efforts to prevent such a breach happening again. In early March, the company announced it would exit some parts of the personal data business and that it would sell information only in situations where specific criteria are met. The transition would be substantially completed

within 90 days, ChoicePoint said at the time. That schedule would mean the effort would be done about early June. On Friday, June 24, ChoicePoint spokesperson Kristen McCaughan said the Alpharetta, GA-based data broker has not yet completed the changes. "It is ongoing," she said. McCaughan could not say when ChoicePoint expects to be able to announce that it has completed the process. "I don't think it is going to be anytime in the near future," she said. One change the company has made, in accordance with federal law, is that consumers can now get a free annual public records report. The report can be requested on the company's ChoiceTrust consumer Website.

Source: http://news.com.com/ChoicePoint+overhaul+falls+behind/2100-1029_3-5761503.html?tag=nefd.top

[[Return to top](#)]

Transportation and Border Security Sector

7. *June 24, USA TODAY* — **FAA: System tracks jets over oceans.** Air traffic controllers will be able to closely monitor jets flying over oceans with a system that should be fully operational by the end of the year, the Federal Aviation Administration (FAA) announced Thursday, June 23. Passengers will see little or no difference. But the system will allow airlines to save millions of dollars in fuel costs by letting planes fly more direct routes over the oceans. The FAA estimates the government and the airlines will save \$2.7 billion by 2013. "This really is an important breakthrough," FAA Administrator Marion Blakey said. "You've got a combination of safety and efficiency in a package." Because there's no radar over the oceans, controllers are unable to get a precise fix on where planes are located. Pilots have for decades had to radio their position once every 50 minutes. Controllers then keep track of planes manually using pieces of paper. The FAA's new system, known as Advanced Technologies and Oceanic Procedures, is a giant step forward, said Dave Ford, the FAA official who oversees it. A device in the cockpit automatically notifies FAA computers where a jet is located. This gives controllers more precise information about each plane's location.

For additional information about Advanced Technologies and Oceanic Procedures:

http://www.faa.gov/airports_airtraffic/technology/atop/

Source: http://www.usatoday.com/travel/flights/2005-06-23-faa-ocean-tracking_x.htm

8. *June 24, Los Angeles Times (CA)* — **Four near misses reported at Los Angeles International Airport.** Aircraft at Los Angeles International Airport (LAX) came too close four times in the last month, a spate of incidents that officials attributed to human error and a record number of international flights. In the most serious recent event, which occurred Sunday, June 19, at 9:45 p.m. (PDT), the pilot of a United Express jet bound for Santa Barbara, CA, had to abort his takeoff and slam on his brakes after a Continental Express jet moved too close to the runway. Controllers told the Continental Express pilot, who had just landed on the outer runway on the airport's south side, to stop behind several sets of "hold bars" painted on a taxiway at midfield. He correctly repeated the instruction to controllers. Then controllers cleared the United Express plane for takeoff on the inner runway. Moments later, they saw the Continental Express jet pass over the hold bars and stop about 39 feet from the edge of the runway. They ordered the United Express pilot to abort his takeoff. The United Express plane skidded to a halt by the Continental jet, with just 100 feet between them. Near misses between aircraft have declined since airport officials launched an intensive campaign to educate pilots about the challenges posed by the

airport's unique layout.

Source: http://www.latimes.com/news/local/la-me-lax24jun24.0.3560694_story?coll=la-home-local

9. *June 24, New York Times* — **Global group backs antiterror customs standards.** The World Customs Organization voted Thursday, June 23, in Brussels, Belgium, to endorse comprehensive standards intended to fight terrorism, a step that United States officials predict will revolutionize the way goods are tracked as they move around the globe. More than 50 nations immediately agreed to put the standards into effect. Under the standards, cargo containers will at times be inspected by customs officials as they leave a port, instead of at their destination. In addition, private importers will get preferred customs handling in return for tightening security to prevent terrorists from using their containers to transport banned weapons. The vote came at a meeting of the group, an association of 166 leaders of customs departments worldwide that collectively handle about 98 percent of international trade. Its members endorsed a set of nonbinding standards, and the group hopes each nation will take on the expense of putting them in place, said Michel Danet, its secretary general. The countries that made immediate commitments to honor the standards include the United States, Mexico, Canada, Japan, China and Brazil, said Robert C. Bonner, commissioner of the United States Customs and Border Protection agency, who helped draft the plans. Department of Homeland Security Secretary Chertoff's remarks on the World Customs Organization vote: <http://www.dhs.gov/dhspublic/display?content=4551> For further information see: http://www.cbp.gov/xp/cgov/newsroom/commissioner/messages/us_joins_wco_std.xml Source: <http://www.nytimes.com/2005/06/24/politics/24customs.html>

10. *June 24, Knight Ridder* — **Illegal immigrants with Hazmat licenses held in fraud probe.** A federal crackdown on fraud at state motor vehicle departments across the country has apprehended more than a dozen illegal immigrants licensed to transport hazardous materials. While none of those apprehended has any known links to terrorism, federal agents said on Thursday, June 23, that the recent arrests have revealed a significant threat to homeland security. In one case, a Pakistani man ordered to leave the United States nine years ago was instead driving a tanker truck filled with gasoline for Exxon. "This is a national security issue," said Elissa Brown, the special agent in charge of the Bureau of Immigration and Customs Enforcement's office in Chicago, where six men were taken into custody. The Department of Homeland Security has begun deportation proceedings against the six illegal immigrants who had obtained commercial drivers' licenses that allowed them to carry hazardous materials. The men are from Belize, Jordan, Mexico, Mongolia and the Philippines. Many states have strengthened their hazardous materials license screening since the September 11, 2001, terrorist attacks. However, state laws remain inconsistent, and Customs says it remains relatively easy to obtain fraudulent documents that can be used to get a driver's license. Source: <http://www.nj.com/news/ledger/index.ssf?/base/news-1/1119596281164070.xml&coll=1>

11. *June 24, Customs and Border Protection* — **Container security initiative for Port of Shenzhen is operational.** On Friday, June 24, United States Customs and Border Protection (CBP) Commissioner Robert C. Bonner and Mu Xinseng, Minister of the General Administration of Customs of the People's Republic of China, announced that the port of

Shenzhen will be the 37th operational port to join the Container Security Initiative (CSI), targeting and pre-screening maritime cargo containers destined for U.S. ports. Under the Container Security Initiative, CBP has entered into bilateral partnerships to identify high-risk cargo containers before they are loaded on vessels destined for the United States. Today, a total of 23 administrations have committed to join CSI and are at various stages of implementation. CBP will deploy a team of officers to be stationed at the port of Shenzhen to target maritime containers destined for the United States. Shenzhen Customs officials, working with CBP officers, will be responsible for screening any containers identified as a potential terrorist risk. Currently, there are 37 operational CSI ports in Europe, Asia, Africa, the Middle East, and North America. CSI will continue to expand to strategic locations around the world. The World Customs Organization (WCO), the European Union (EU), and the G8 support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world.

Source: http://www.cbp.gov/xp/cgov/newsroom/press_releases/06242005.xml

12. *June 23, Department of Transportation* — **Rail safety research grant funds field testing for train collision prevention technology.** A technology designed to prevent train collisions and other types of rail accidents moves another step forward on Thursday, June 23, thanks to a \$6.4 million grant from the Federal Railroad Administration (FRA). The grant to the Railroad Research Foundation in Washington, DC will help fund the completion of field testing of a Positive Train Control (PTC) system. PTC technology improves rail safety by automatically keeping trains within track speed limits, helping to identify trains and other obstructions on the track ahead, and bringing a train to a stop if the engineer fails to take corrective action when warned of a safety hazard. The field testing consists of a full scale operation on a 120 mile segment of track between Springfield, IL, and St. Louis, MO, involving both a freight and passenger train to verify the proper and complete transmission of electronic data between equipment on board the locomotives, along the tracks, and from the dispatch center to safely and automatically control the movement of the trains. Boardman noted the future capabilities of PTC systems, which can potentially make highway-rail grade crossings safer by giving motorists in-vehicle advance warning of the approach of a train.
- Source: <http://www.dot.gov/affairs/fra1305.htm>

13. *June 23, Department of Transportation* — **New grants to fund research to reduce track caused train accidents.** The Federal Railroad Administration (FRA) on Thursday, June 23, announced the award of two rail safety research grants to universities in Alabama and Illinois intended to improve safety in the railroad industry. Specifically, Tuskegee University received \$96,192 to study the effect of fatigue on different types of rail steel and to identify how rail fractures develop and spread. The University of Illinois at Chicago received \$166,610 to create software that can study derailments, wheel/rail contact in three dimensions, and rail car dynamics under higher speeds of operation. These research grants support the FRA's National Rail Safety Action Plan that targets the most frequent, highest risk causes of accidents. Track-caused accidents are the second leading cause of all train accidents. While the rail industry experienced a reduction in the overall number of track-caused accidents in recent years, heavier freight car loads and the continued growth of rail traffic increases track stress and fatigue. FRA also is sponsoring research on technologies that alert train crews to broken rails before they approach them, and on the composition and construction design of railroad cross-ties that keep the rail in place and properly aligned.

Source: <http://www.dot.gov/affairs/fra1405.htm>

[\[Return to top\]](#)

Postal and Shipping Sector

14. *June 24, Postal Service* — U.S. Postal Service offers premium forwarding service details.

The U.S. Postal Service (USPS) has released Domestic Mail Manual standards for its Premium Forwarding Service (PFS) experiment. The USPS is conducting this nationwide, two-year experiment starting August 7 to measure interest in a new service that ships mail to residential customers who are away from their main address for at least two weeks and up to one year. PFS provides a shipment of a customer's mail every Wednesday from their main address to their temporary address by Priority Mail service. The service differs from two services USPS currently offers: Temporary Forwarding, which forwards certain types of mail to a temporary address on a piece-by-piece basis; and Hold Mail, under which all mail for an entire household can be held at the post office for up to 30 days. For PFS, customers pay an initial enrollment fee of \$10 plus a weekly per-shipment charge of \$10. Express Mail and Priority Mail packages that are too large to fit inside the weekly PFS package are immediately and separately rerouted at no additional charge. Package Services parcels that are too large to fit inside the PFS package are rerouted with postage due. All mail requiring a delivery scan or a signature also is separately rerouted.

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=33189

[\[Return to top\]](#)

Agriculture Sector

15. *June 25, Associated Press* — U.S. seeks source of mad cow infection. The U.S. Department of Agriculture's (USDA) hopes DNA analysis can pinpoint the herd of the cow that tested positive for mad cow disease and lead investigators to the source of the animal's brain-wasting illness. Genetic testing is needed because of mistakes in how the beef cow was labeled and how its tissues were stored, John Clifford, chief USDA veterinarian, told The Associated Press. The cow, a "downer" that could not walk, was delivered last November to a plant where animals unfit for human consumption are killed. The cow's type of breed was mislabeled, and its tissues were mixed with tissues from other cows, Clifford said. "When we went back to this particular owner, the breed we identified, he indicated he did not sell that breed. He sold another breed," Clifford said. "In addition to that, we found that after the tissues were processed, there was some mixing." Parts from the diseased animal and four other cows were supposed to be kept in separate waste barrels, but some of the waste was combined, Clifford said. USDA officials think they have found the right herd. To confirm that, they must find relatives of the dead cow and test DNA. Finding the herd will help track the cow's feed and explain how the animal became infected.

Source: <http://apnews.myway.com/article/20050625/D8AURRT00.html>

16. *June 24, Agricultural Research Service* — Manual highlights arthropods that curb aquatic weeds. A manual developed by the Agricultural Research Service (ARS) and now available

online helps scientists, resource managers and others identify biological control insects that play a key role in helping to control aquatic weeds. The importance of these plant-feeding insects to the dynamics of aquatic and wetland ecosystems is the focus of the new, online reference called "Insects and Other Arthropods That Feed on Aquatic and Wetland Plants." The 200-page manual explains the life cycles of more than 50 of the most common insects and mites found in aquatic environments. The manual was originally published by ARS scientists at the Invasive Plant Research Laboratory (IPRL) in Fort Lauderdale, Fla., in cooperation with colleagues from the Florida Department of Environmental Protection and the U.S. Army Corps of Engineers. The IPRL mission is to address the complex, multifaceted problems caused by the invasion of natural and agricultural ecosystems by exotic species. Non-native plants pose some of the most serious threats to the health and integrity of these ecosystems, according to Ted D. Center, IPRL research leader.

Online Manual: <http://www.ars.usda.gov/is/np/aquaticweeds/aquaticweedsintro.htm>

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

17. *June 24, USAgNet* — **Alert level raised for Louisiana soybean growers.** A University of Arkansas plant pathologist, reported the presence of spores like those associated with Asian soybean rust in St. Joseph, LA, where they were captured by a spore trap. Monitored by Louisiana State extension specialists, the spore trap in Tensas county, located near the Louisiana border between Natchez, MS, and Vicksburg, MS, tested positive for the presence of three spores associated with soybean rust. Utilizing technology developed for rust detection in Brazil and Paraguay, spore traps are custom-designed traps monitored by trained pathologists to detect rust spores in the area. Spore traps are able to detect spores in the air and collect samples for lab analysis. The Syntinel trap network, exclusive to Syngenta, consists of nearly 100 traps across the country, with an early-season emphasis in the southern soybean-growing areas of the U.S. By capturing windborne spores, the Syntinel traps can provide an early alert system of the potential of rust development in a specific area.

Source: <http://www.usagnet.com/story-national.cfm?Id=646&yr=2005>

18. *June 24, Palm Beach Post (FL)* — **Survey of commercial groves to determine spread of canker.** State and federal officials will launch a fresh survey Monday, June 27, of Florida's commercial fruit groves in an attempt to get hold of the citrus canker crisis that has been plaguing the state for 10 years. About 100 U.S. Department of Agriculture (USDA) canker inspectors who normally would be looking for the disease in residential areas will instead be going to work in the commercial groves. The new inspections follow news that the state is about two months behind on its commercial canker survey because of the large number of outbreaks that appeared on the heels of last year's hurricanes. State and federal officials said the bulk of the areas most obviously impacted by the hurricanes have been checked for signs of the bacterial disease. The new survey, which should take two months to complete, is aimed at finding out whether canker has spread farther. Tim Riley, a USDA plant pathologist in Orlando who is involved in the project, said the state's canker program has reached the point where there's a need for an updated assessment. If the rate of infection is faster than the rate of tree removal, it could become difficult to keep up, he said.

Source: http://www.palmbeachpost.com/business/content/business/epaper/2005/06/24/a1d_canker_0624.html

19.

June 24, Seattle Times (WA) — **Japan's import barriers on U.S. apples ruled illegal.**

Washington and Oregon apple growers won a 20-year trade battle Thursday, June 23, when the World Trade Organization (WTO) ruled Japan's import barriers to U.S. apples are illegal. The decision requires Japan to admit U.S. apples, a potential market estimated at \$143.4 million a year, or face U.S. trade sanctions. The decision is expected to help open markets in other countries with similar restrictions. In the trade case, Japan claimed importing U.S. apples would expose its orchards to fire blight, a bacterial disease endemic in the U.S. But a WTO panel found Japan's import requirements for U.S. apples lacked scientific backing, and were too restrictive on trade. Japan required U.S. apples to come from orchards with 500-yard buffer zones on all sides and three inspections a year. The WTO decision could open up U.S. exports to Australia, South Africa, and China, for certain varieties of apples, which are now restricted because of fire-blight concerns.

Source: http://seattletimes.nwsources.com/html/business/technology/2002346500_apples24.html

20. *June 24, Computer World* — **U.S. lags in effort to create animal ID system.** An automated national system for tracking animals faces countless challenges and is still years away from being operational. Though the U.S. Department of Agriculture (USDA) has been actively working on a program since 2003, the U.S. continues to lag behind beef producing rivals such as Japan, Australia, or the United Kingdom. The project, dubbed the National Animal Identification System (NAIS), was officially launched after the discovery of a case of mad cow disease in Washington in 2003. The USDA has set a July 6 deadline for public input as it drafts a strategic plan and program specifications. So far, users question whether the project is adequately funded and express concern about the ability to choose the right technology for the effort. Although there is no official estimate, some observers have pegged the long-term cost of the NAIS project at \$600 million-plus. Currently, a fully operational system is slated to be online in 2009, when participants will be required to have both their premises and animals logged into a national database that will enable a complete trace within 48 hours.

Source: <http://www.computerworld.com/government/government/policy/story/0,10801,102754,00.html>

[[Return to top](#)]

Food Sector

21. *June 24, USAGNet* — **Alaska to label biotech fish.** A new Alaskan law requiring a special label for genetically modified fish is on the cutting edge of national efforts to regulate biotechnology in the food chain. The law was passed primarily to protect the state's fishing industry, which has suffered from the growth of fish farming. Supporters also call it a breakthrough in alerting consumers about what they are eating. While European countries have required labels for all genetically modified foods since 1998, similar proposals have failed in California, Maine, Michigan, Oregon, and Vermont over the past decade. Under Alaska's law, which passed this session with unanimous support, a label must inform buyers that a fish or fish product has been genetically altered "by means that are not possible under natural conditions or processes."

Source: <http://www.usagnet.com/story-national.cfm?Id=645&yr=2005>

[[Return to top](#)]

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

22. *June 26, San Mateo Times (CA)* — California unprepared for terror or epidemic, commission says. Despite some progress, California remains in many ways unprepared for a large epidemic or terrorist attack, with no method of watching for a fast-moving disease, the Little Hoover Commission said. There is no clear state plan for mobilizing large numbers of medical personnel, distributing drugs, or communicating among first responders and health workers, the commission said. Most of all, the commission said that California needs a state Department of Public Health to prepare for a large-scale health crisis. Public health experts say without clear state leadership, California will be outpaced by a fast-spreading outbreak, at a needless cost in lives. The commission concluded the state's Department of Health Services hasn't been up to the task and largely has neglected public health because the agency is consumed with running Medi-Cal, the health insurance program serving six million Californians. The findings of the commission, a bipartisan panel overseeing state government for the governor and the legislature, echo earlier reports by the Santa Monica think tank Rand and Governor Arnold Schwarzenegger's California Performance Review of state government. All recommended creating a separate public health department.

Source: http://www.insidebayarea.com/sanmateocountytimes/localnews/c_i_2825633

23. *June 24, Reuters* — Experts in Vietnam to study bird flu evolution. A team of international experts is in Vietnam studying whether the H5N1 bird flu virus may be evolving into a form that might trigger a human pandemic, the World Health Organization (WHO) said on Friday, June 24. The team of virologists and epidemiologists was looking at "the possibility of more widespread H5N1 human transmission, changes in the H5N1 virus and the likelihood of increased human-to-human transmission," the WHO said. "What has happened in Vietnam may have public health implications for the entire world and will be crucial in preparing for a possible pandemic," said Hans Troedsson, WHO Representative in Vietnam. Scientists have been tracking the evolution of the H5N1 virus, which is infectious in birds but does not spread easily among humans. However, the fear is that it could mutate into a form that spreads easily among people, unleashing a pandemic. So far, there have been very few cases in which human-to-human transmission is suspected. Last week, a Vietnamese doctor who treated bird flu patients tested positive for the virus, but the Health Ministry insisted there has been no evidence of human-to-human transmission of the virus in Vietnam so far.

Source: <http://www.alertnet.org/thenews/newsdesk/HAN146324.htm>

[\[Return to top\]](#)

Government Sector

24.

June 24, Government Accountability Office — **GAO-05-790: Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism (Report).** The threat of terrorism has made physical security for federal real property assets a major concern. Protecting these assets can be particularly complex and contentious for agencies whose missions include ensuring public access such as the Department of the Interior (Interior) and the General Services Administration (GSA). The Government Accountability Office (GAO)'s objectives were to (1) identify any challenges that Interior faces in protecting national icons and monuments from terrorism, as well as related actions intended to address these challenges; and similarly, (2) determine any challenges GSA faces related to the protection of federal office buildings it owns or leases and actions that have been taken. GAO recommends that the Secretary of the Interior (1) link the results of its risk assessments and related risk rankings to its funding priorities, and (2) develop guiding principles for balancing security initiatives with Interior's core mission. Interior did not comment on the recommendations. GAO also recommends that the Administrator of GSA establish a mechanism — such as a chief security officer position or formal point of contact — so it is better equipped to address security related matters related to its federal building portfolio. GSA concurred with the recommendation.

Highlights: <http://www.gao.gov/highlights/d05790high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-790>

25. *June 24, Associated Press* — **University of Connecticut offering master's degree in homeland security.** A new program at the University of Connecticut (UConn) will offer a master's degree in homeland security. At least 70 students have applied for the expected class of 25 for the program this fall, which UConn is offering in partnership with the Naval Postgraduate School in Monterey, California. "Business and industry are looking for a curriculum that prepares them for the same kinds of things government employees are being trained for," said Krista Rodin, dean of UConn's College of Continuing Studies. "This is an emerging field," Rodin said. "We do not have a curriculum like this anywhere in the country." The program is aimed at working adults in both the public and private sector. Students will learn how to respond to disasters such as outbreaks of diseases or terrorist attacks that endanger food supplies. Students spend five weeks of the 20-month program at UConn's main campus in Storrs. The rest of the program will be done online.
- Source: <http://www.cnn.com/2005/EDUCATION/06/24/homeland.security.ap/index.html>

[\[Return to top\]](#)

Emergency Services Sector

26. *June 24, Daily Republic (CA)* — **Preparing for terror: California county agencies work together for drill.** The Solano County Office of Emergency Services teamed up with a host of police and fire departments, Travis Air Force Base, and health agencies to put the county's ability to deal with a hazardous materials spill to the test. More than a dozen agencies ranging from Vallejo to Dixon with about 200 police, firefighters, security forces, paramedics, and explosives disposal experts took part on Friday, June 24. The drill tested the agencies' ability to deal with a criminal attack that released hazardous materials in a residential area, injuring a large number of people. This was the first such multi-agency drill since November 2003, when more than 300 police and firefighters participated in a nighttime exercise to find out how to

work together better.

Source: http://www.dailyrepublic.com/articles/2005/06/25/local_news/news05.txt

- 27. June 24, WTOC (GA) — Segway scooters help bomb squad.** The Savannah–Chatham, GA, bomb squad and Hazmat crews say new technology could be a huge help in their efforts: Segway scooters. The bomb squad gets 120 bomb calls a year and these human transporters would make life for them a lot easier. The safe distance for the bomb squad is 1,000 feet from the bomb or suspicious package. For example, in a recent drill, instead of walking back and forth as many as 6,000 feet, Sgt. Rob Von Loewenfeldt used a Segway. Once he located the bomb, Sgt. Von Loewenfeldt realized he needed to make another trip. So he headed back to the bomb team, another 1,000–foot trip. "If I had to walk that, it would have been like double the distance, twice as hard. Savannah Fire Department's Hazmat team has its eyes on the Segway too. The department's Shaw Newton had no problems testing out the technology. "In case of an emergency, it would be worth it." Lt. Bud Pierce says Segways would reduce risks of dehydration and exhaustion, and let bomb techs work longer.

Source: http://www.wtoctv.com/Global/story.asp?S=3518623&nav=0qq6bQy_n

- 28. June 24, Associated Press — Dogs in Birmingham K–9 unit sniff for bombs at airport.** Routine explosive detection training sessions are run at least twice a week by the Birmingham, AL, Police Department's K–9 explosive detection unit. The force, responsible for sweeping the airport and responding to bomb threats, will double in size by summer's end with the addition of two additional dogs and officers. Transportation Security Administration (TSA) spokesperson Chris White said, "It is not an overstatement by saying this (addition) directly makes the public safer," said White, adding that dogs are the quickest and most accurate way to detect explosives. Trained dogs search planes and luggage and do routine sweeps of the concourses. They can sniff out 11 different explosives, including dynamite, C–4 and Semtex, which Birmingham Police Officer David Hale said is currently "the explosive of choice." TSA–trained dogs correctly identify explosives 96 percent of the time, he said. That's quite an accomplishment, he said, considering that the 11 types of explosives also smell different depending on their weight.

Source: <http://www.jedger-enquirer.com/mld/jedgerenquirer/news/local/11986057.htm>

[[Return to top](#)]

Information Technology and Telecommunications Sector

- 29. June 24, BBC News — Computer passwords 'up for grabs' according to IT security firm.** Half of IT managers employed by large–sized companies believe it would be relatively easy to gain the core passwords for their computer systems. That is the warning of a survey by IT security firm, Cyber–Ark. It said that ten percent of firms never changed their central administrative passwords. A further five percent did not even bother altering the manufacturer's default password that came with the system. The survey also found one IT boss who kept all passwords on his mobile phone. Less than a third of IT managers store key passwords digitally, the survey of 175 IT professionals revealed. The remainder continued to keep paper copies, stored everywhere from locked cabinets to safes. About 25% of IT staff could, as a result, access the core passwords without official permission, the survey said. The survey found that IT managers estimate 19% of general staff in their firms still keep their passwords on notepaper

beside their computers.

Cyber–Ark Press Release: http://www.cyber-ark.com/networkvaultnews/pr_20050608.htm

Source: <http://news.bbc.co.uk/1/hi/business/4618691.stm>

30. *June 24, Newsfactor Network* — **Sandia develops secure ultrawideband wireless network.** A group led by researchers at Sandia National Laboratories has developed a wireless network based on wavelengths in the ultrawideband spectrum. Ultrawideband—called UWB or, alternately, "impulse radio"—is different from other kinds of wireless transmissions because it does not use a carrier. Instead, UWB transmits a flood of very short microwave pulses of energy on the order of 100 picoseconds. These pulses extend over an extremely wide band of radio energy that covers several frequencies in the radio spectrum. The network, said Sandia, is secure enough to be used for national–defense purposes, to help sensors monitor U.S. Air Force bases or Department of Energy nuclear facilities, for example. It also could be used to control remotely operated weapon systems wirelessly. One level of protection is provided by encryption, said lab spokesperson Michael Padilla. Another comes from the fact that signals over UWB are difficult to distinguish from background radio frequency noise in general "...and when combined with [encryption], virtually impossible to crack," said H. Timothy Cooley, senior scientific engineer at Sandia. The newly developed network, said the researchers, is capable of high–level encryption up to and beyond 256 bits, which is currently double the amount considered essential for secure Internet transactions.

Source: http://news.yahoo.com/s/nf/20050623/tc_nf/36740;_ylt=ApQZyLu

[WFTn_aT81drbhp20jtBAF;_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCU](http://news.yahoo.com/s/nf/20050623/tc_nf/36740;_ylt=ApQZyLuWFTn_aT81drbhp20jtBAF;_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCU)

31. *June 24, SecurityFocus* — **Veritas Backup Exec/NetBackup request packet denial of service vulnerability.** VERITAS Backup Exec and NetBackup for NetWare Media Servers are prone to a denial of service vulnerability. A malformed request packet may cause a denial of service on the computer hosting the application. Updates available:

<http://www.securityfocus.com/bid/14019/references>

Source: <http://www.securityfocus.com/bid/14019/solution>

32. *June 24, SecurityFocus* — **Veritas Backup Exec Remote Agent null pointer dereference denial of service vulnerability.** VERITAS Backup Exec Remote Agent is prone to a remotely exploitable denial of service vulnerability. This flaw is due to an error in the handle used by the application, which could be exploited by non–privileged users to execute arbitrary commands with SYSTEM privileges. Updates available through Source link below.

Source: <http://www.securityfocus.com/bid/14021/solution>

33. *June 23, FrSIRT* — **Veritas Backup Exec Web Administration Console (BEWAC) vulnerability.** A vulnerability was identified in Veritas Backup Exec Web Administration Console (BEWAC), which could be exploited by remote attackers to gain unauthorized access. This flaw is due to a buffer overflow error when processing specially crafted authentication requests, which can be exploited by remote unauthenticated attackers to execute arbitrary commands. Updates available: <http://support.veritas.com/docs/276606>

Source: <http://www.frsirt.com/english/advisories/2005/0855>

34. *June 23, FrSIRT* — **Multiple DUware products remote SQL injection vulnerability.** A vulnerability was identified in various DUware products, which may be exploited by remote

attackers to execute arbitrary SQL commands. This flaw is due to an input validation error when processing specially crafted parameters, which may be exploited by remote users to conduct SQL injection attacks. There is no solution at this time.

Source: <http://www.frsirt.com/english/advisories/2005/0863>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT has received reports of the existence of a working exploit for a recently published vulnerability in Microsoft Outlook Express. While reports of successful system compromise using this vulnerability have not yet been confirmed, US-CERT urges users to review the information in US-CERT Vulnerability Note: VU#130614 – Microsoft Outlook Express vulnerable to remote code execution Microsoft has released a patch to address this vulnerability in Microsoft Security Bulletin MS05-030.

US-CERT has received some reports about spikes on port 10000. The release of the exploit for Veritas, used by the Metasploit Framework seems to be responsible. An excerpt of the exploit

(http://www.frsirt.com/exploits/20050625.backupexec_agent.pm.php) is below:
'RHOST' => [1, 'ADDR', 'The target address'], 'RPORT' => [1, 'PORT', 'The target port', 10000], For more information, please see <http://isc.sans.org//index.php>

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 27015 (halflife), 41170 (----), 1026 (----), 4672 (eMule), 6881 (bittorrent), 53 (domain), 32775 (sometimes-rpc13), 139 (netbios-ssn) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

35.

June 25, Reuters — **Algeria jails Islamic militant for life.** One of Algeria's top Islamic rebels, wanted in Germany for the kidnapping of 32 European tourists in the Algerian Sahara desert in 2003, was sentenced to life in prison in his absence on Saturday, June 25 for helping to create a terrorist group. Amari Saifi, deputy head of the al Qaeda aligned Salafist Group for Preaching and Combat (GSPC), was convicted in a court in the capital Algiers of creating an armed terrorist group and spreading terror among the population. The GSPC is blamed for the killings of thousands of soldiers and civilians since its creation in 1998 to overthrow the authorities and set up a purist Islamic state. Saifi, a former army paratrooper, was tried in his absence as the case was brought to the court before his extradition to Algeria last October. The authorities have said he is in custody at an undisclosed location and under interrogation for other terrorism-related charges. Local media have questioned the whereabouts of Saifi but security experts say that give the number of terrorism cases he is linked to, and national security-sensitive information he is believed to hold, the authorities are reluctant to bring him before the courts for each case.

Source: <http://www.reuters.com/newsArticle.jhtml?type=worldNews&storyID=8892430>

[\[Return to top\]](#)

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983-3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.